UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/452,329	11/30/1999	GARY L. GRAUNKE	42390.P7947	1161

7590 05/24/2004

ALOYSIUS T C AU YEUNG
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
12400 WILSHIRE
7TH FLOOR
LOS ANGELES, CA 90025

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	**PAPER NUMBER**
2131	8

DATE MAILED: 05/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/452,329	GRAUNKE ET AL.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 March 2004*.

2a)☐ This action is **FINAL**. 2b)☐ This action is non-final.

3)☒ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) *1-21* is/are withdrawn from consideration.

5)☒ Claim(s) *22-41* is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 March 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment filed on 04 March 2004 is noted and made of record.

2. Claims 1-41 are presented for examination.

3. Claims 1-21 have been cancelled as per Applicant's request.

Drawings

4. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: 302. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Allowable Subject Matter

5. Claims 21-41 are allowed.

6. The following is an examiner's statement of reasons for allowance:

As per claim 22, it is well known in the art for an apparatus to produce a pseudo random sequence, comprising: a data bit generator to produce a principal data stream; multiple data bit generators to create additional data streams; a storage structure responsive to the additional data streams having multiple bit storage locations to store the bits of the principal data stream; and a shuffle unit coupled with the data bit generators to modify the principal data stream by combining the bits of the principal data stream with past bits of the principal data stream stored in the storage structure.

There are no teachings in the prior art of storing the principal data stream in the storage locations in a pseudo random order based on an order of bits in the additional data streams (Emphasis added). Furthermore there is no teaching of combining the bits of the principal data

stream with past bits of the principal data stream stored in the storage structure and pseudo randomly selected from the storage structure based on an order of the bits in the additional data streams to produce a pseudo random sequence (Emphasis added). Since no teachings or motivation can be found of the abovementioned limitations, claim 22 is therefore novel and non-obvious.

As per claim 29, it is well known for a method to generate a data stream, comprising: generating a first and a second bit sequence; storing bits from the first sequence in a memory structure; retrieving stored bits of the first sequence from the memory structure; bit-wise modifying the bits of the first sequence with the stochastically retrieved bits to produce a pseudo random data stream.

There is no teaching in the prior art of retrieving stored bits of the first sequence from the memory structure in a stochastic order, the order based at least in part on a bit order of the second sequence (Emphasis added). Since no teachings or motivation can be found of the abovementioned limitation, claim 29 is therefore novel and non-obvious.

As per claim 35, its is well known in the art for a stream cipher generator comprising: a first data bit generator to produce a first stream of data bits; a memory having a read and write port to receive and store bits from the first stream of data bits; a second data bit generator to produce a second stream of data bits; a read and write port controller coupled to the memory; and a combiner to receive the first stream of data bits and the bits read from the memory, and modify

the first stream of data bits with the bits read from the memory to produce a pseudo random sequence.

There is no teaching in the prior art of a read and write port controller coupled to the memory and responsive to the second stream of data bits, to control the read and write functions of the memory based, at least in part, on the sequence of bits in the second stream of data bits (Emphasis added). Since no teachings or motivation can be found of the abovementioned limitation, claim 29 is therefore novel and non-obvious.

7. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

9. The following patents are cited to further show the state of the art with respect to stream ciphers with a combiner function, such as:

United States Patent No. 4,082,217 to Michener, which is cited to show a method and apparatus for securing access to a computer facility.

United States Patent No. 5,323,338 to Hawthorne, which is cited to show pseudo-random sequence generators.

United States Patent No. 5,566,099 to Shimada, which is cited to show a pseudo-random number generator.

United States Patent No. 5,751,808 to Anshel et al., which is cited to show multi-purpose high speed cryptographically secure sequence generators based on zeta-one-way functions.

United States Patent No. 5,341,425 to Wasilewski et al., which is cited to show a method and apparatus for uniquely encrypting data at a plurality of data transmission sites for transmission to a reception site.

United States Patent No. 5,577,124 to Anshel et al., which is cited to show multi-purpose high speed cryptographically secure sequence generators based on zeta-one-way functions.

United States Patent No. 6,192,385 to Shimada, which is cited to show a pseudo-random number generator.

United States Patent No. 5,598,154 to Wilson et al., which is cited to show generating and utilizing pseudo-noise code sequences.

10. This application is in condition for allowance except for the following formal matters:

The Objection to the Drawings.

11. Prosecution on the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

12. A shortened statutory period for reply to this action is set to expire **TWO MONTHS** from the mailing date of this letter.

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (703) 305-7704. The examiner can normally be reached on Monday thru Thursday 7-5.

14. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

15. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131

clf

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100